

GREYCORTEX

AI ve službách bezpečnostního monitoringu sítí

CO JE GREYCORTEX?

Společnost: GREYCORTEX s.r.o., Brno

- 100% český kapitál, profesionálové v IT a veteráni kyberbezpečnosti (C|EH, CISSP, ...)

Cíl: Pomáhat ochraně podniků, úřadů, kritické infrastruktury, výroby a provozu gridů

- Prostřednictvím sledování a analýzy provozu IT a OT (SCADA, ICS, Smart Buildings / Cities / Grids)

Produkt: GREYCORTEX MENDEL

- kombinace BI, ML a AI

Historie: 2009 výzkum (analýza bezp. videozáznamů - 3x cena NIST)
2013 produkt pro NTA (MENDEL)
2016 založen GREYCORTEX
2016+ spolupráce s univerzitami a dalšími (CCD COE)
2017 člen ESET Technology Alliance

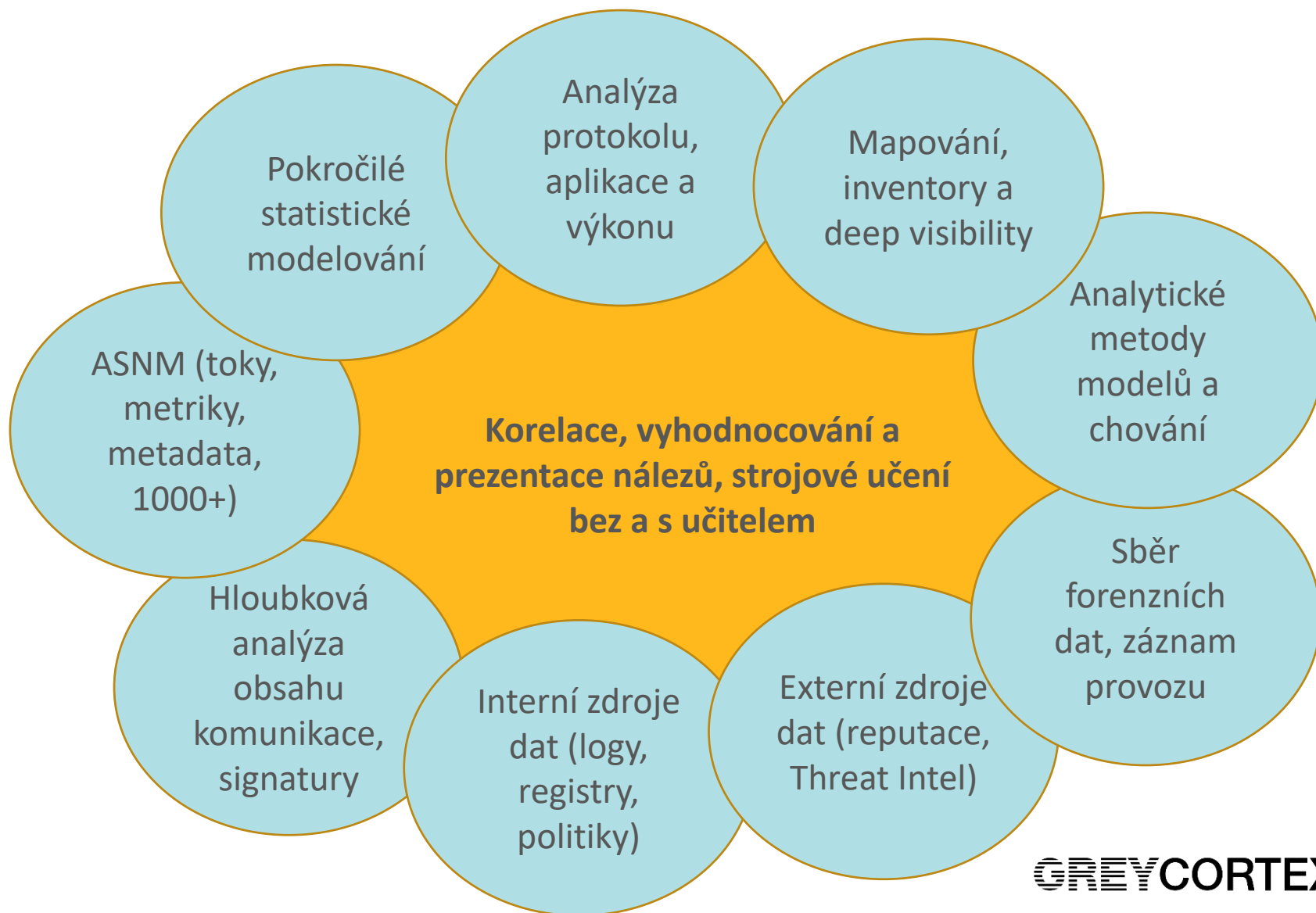
Gartner Market Guide for Network Traffic Analysis 2019:
jediný dodavatel NTA v kontinentální Evropě

GREYCORTEX

MENDEL: Posvit' na síť!

Plná síťová viditelnost a analýza dostupných dat pro síťovou bezpečnost

ZDROJE A SOUČÁSTI ANALÝZY PROVOZU



ZÍSKÁVÁNÍ A OBOHACOVÁNÍ DAT

Senzor: Zrcadlo provozu

- SPAN / mirror port
- TAP na lince
- Packet broker

Senzor: Automatické využití provozních informací z monitorované sítě

- DNS/DHCP
- Služby, klasifikace rolí zařízení

Konfigurace systému (při uvádění do provozu a změnách)

- Politiky, segmentace sítě a další

Kolektor: Příjem dat ze sítě

- ASNM, NETFLOW 5+, IPFIX a další
- rsyslog

Kolektor: Aktivní dotazování

- LDAP/AD
- Reputační služby

GREYCORTEX agregátor

- Signatury (Open source, komerční)
- Registry
- Aktualizace

AUTOMATICKÁ A ASISTOVANÁ REAKCE

Integrační pluginy pro řízení firewallů a NAC

- Známí výrobci, obecné řízení
- Přizpůsobení konkrétnímu prostředí
 - Zastavení na firewallu
 - Přepojení do karantény

Zavedení a aktivace omezení provozu

- Automaticky při detekci (s následným potvrzením / zamítnutím)
- Manuálně operátorem (potvrzení nálezu)

MENDEL: Co vidíš?

Plná síťová viditelnost a analýza dostupných dat pro síťovou bezpečnost

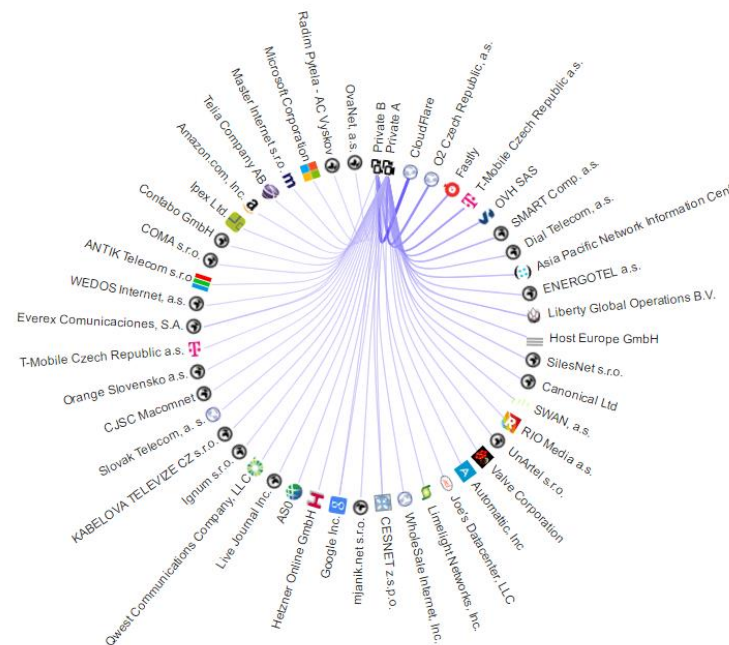
VIDITELNOST: NAJDI, ZAPIŠ A MODELUJ

Sít'

- Inventory: Umístění, Adresy, ASN, Lokace
- Model: Čas, síť, služby, metriky

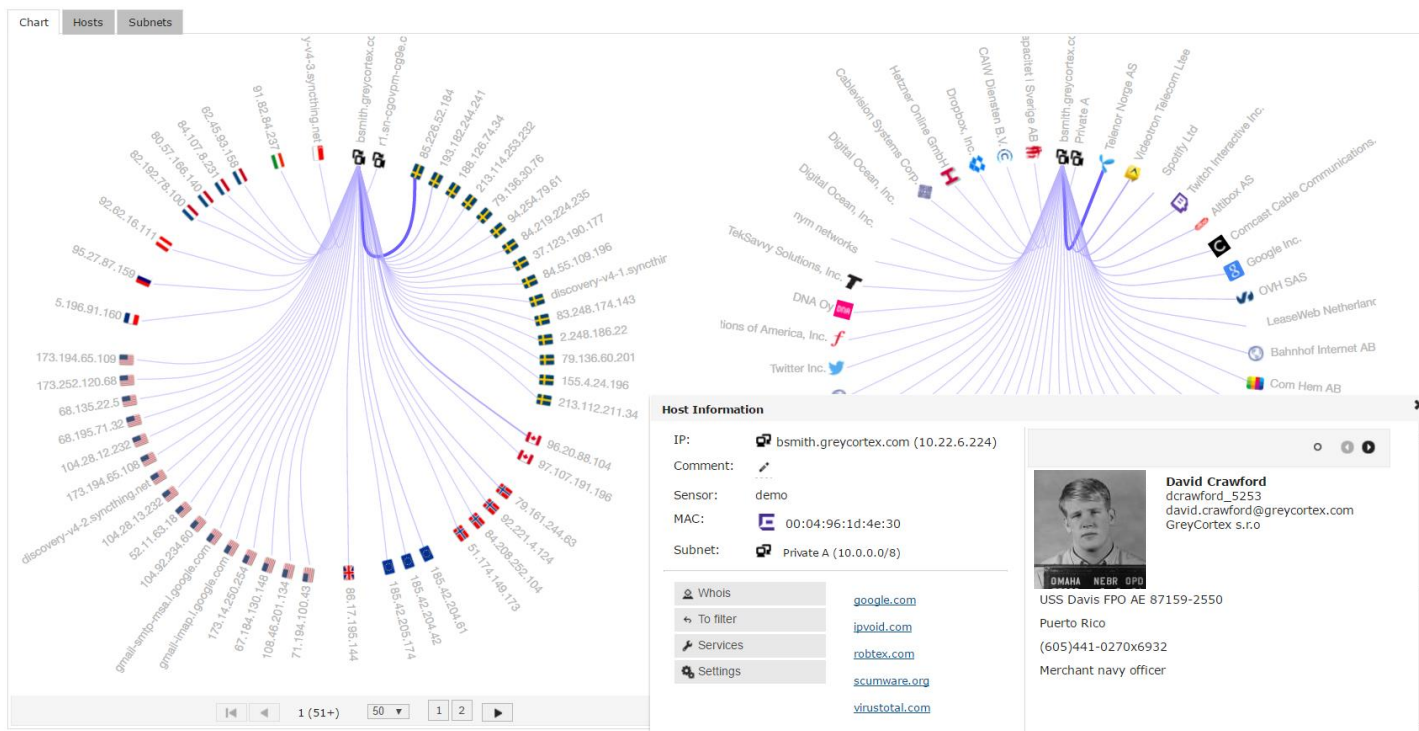
Koncové zařízení

- Inventory: Umístění, Adresy, Služby, Protokoly
- Model: Čas, síť, služby, protokoly, metriky
- Automatické zjištění nových zařízení a služeb
- Pouze pomocí monitoringu, analýzy a učení (nenastavuje se ručně!)



... PŘI ANALÝZE

S kým se tenhle týpek baví?



DETEKUJ: ANOMÁLIÍ, HROZBU, VÝPADEK

Předpověď příští hodnoty sledovaného ukazatele

Nečekaně vysoká nebo nízká, strojově periodická

Hlubková inspekce paketů

Signaturní detekce

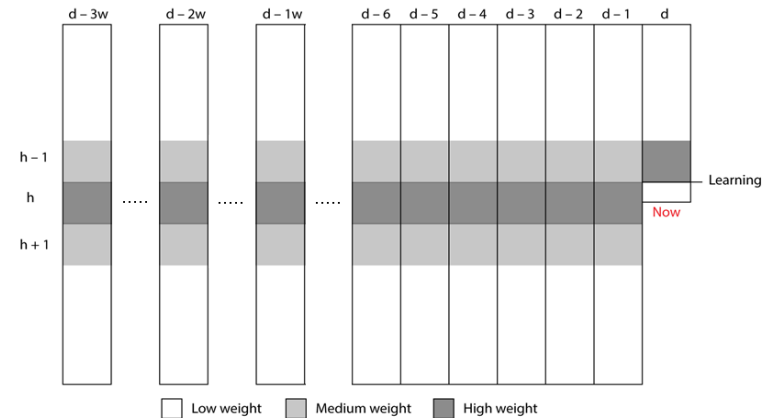
Korelace indikátorů rizik a anomálií

Profilování aplikačních dialogů

Výkon, latence, saturace

Supervizované strojové učení

Doladění citlivosti na odchylky ukazatelů



... PŘI ANALÝZE

Skenování portů ve vnitřní síti – rekognoskace sítě

8 scan: Internal scan-like behavior ? Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	iData	oData	ΣEvent	Date
10.0.0.100	10.0.0.100	10.0.0.0/24	10.0.0.0/24		TCP (6)	1.57 k	1.57 k		94.32 k		Thu 12:35

Flows	Peers	Reported timestamp:	2016-09-08 12:35:28	2016-09-08 12:37:00	Search	Flip									
Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	RTT [s]	Src Flags	Dst Flags	End Time
10.0.0.100	10.0.0.100	TCP (6)	62848	20		1	60		1	60		S	2016-09-08 12:35:29
10.0.0.100	10.0.0.100	TCP (6)	64672	20		1	60		1	60		S	2016-09-08 12:35:37
10.0.0.100	10.0.0.100	TCP (6)	65393	20		1	60		1	60		S	2016-09-08 12:35:44
10.0.0.100	10.0.0.100	TCP (6)	62884	20		1	60		1	60		S	2016-09-08 12:35:29
10.0.0.100	10.0.0.100	TCP (6)	63318	20		1	60		1	60		S	2016-09-08 12:35:30
10.0.0.100	10.0.0.100	TCP (6)	63263	20		1	60		1	60		S	2016-09-08 12:35:30
10.0.0.100	10.0.0.100	TCP (6)	65186	20		1	60		1	60		S	2016-09-08 12:35:41
10.0.0.100	10.0.0.100	TCP (6)	65269	20		1	60		1	60		S	2016-09-08 12:35:42
10.0.0.100	10.0.0.100	TCP (6)	65428	20		1	60		1	60		S	2016-09-08 12:35:45
10.0.0.100	10.0.0.100	TCP (6)	63692	20		1	60		1	60		S	2016-09-08 12:35:32
10.0.0.100	10.0.0.100	TCP (6)	49265	20		1	60		1	60		S	2016-09-08 12:35:46
10.0.0.100	10.0.0.100	TCP (6)	64872	20		1	60		1	60		S	2016-09-08 12:35:38
10.0.0.100	10.0.0.100	TCP (6)	62968	20		1	60		1	60		S	2016-09-08 12:35:29
10.0.0.100	10.0.0.100	TCP (6)	63866	20		1	60		1	60		S	2016-09-08 12:35:33
10.0.0.100	10.0.0.100	TCP (6)	64642	20		1	60		1	60		S	2016-09-08 12:35:37
10.0.0.100	10.0.0.100	TCP (6)	64937	20		1	60		1	60		S	2016-09-08 12:35:39
10.0.0.100	10.0.0.100	TCP (6)	65245	20		1	60		1	60		S	2016-09-08 12:35:42
10.0.0.100	10.0.0.100	TCP (6)	65225	20		1	60		1	60		S	2016-09-08 12:35:42
10.0.0.100	10.0.0.100	TCP (6)	64966	20		1	60		1	60		S	2016-09-08 12:35:39
10.0.0.100	10.0.0.100	TCP (6)	63171	20		1	60		1	60		S	2016-09-08 12:35:30
10.0.0.100	10.0.0.100	TCP (6)	65376	20		1	60		1	60		S	2016-09-08 12:35:44
10.0.0.100	10.0.0.100	TCP (6)	65492	20		1	60		1	60		S	2016-09-08 12:35:46
10.0.0.100	10.0.0.100	TCP (6)	64834	20		1	60		1	60		S	2016-09-08 12:35:38
10.0.0.100	10.0.0.100	TCP (6)	65032	20		1	60		1	60		S	2016-09-08 12:35:40
10.0.0.100	10.0.0.100	TCP (6)	62593	20		1	60		1	60		S	2016-09-08 12:35:28

DOKUMENTUJ: ZACHYCENÝ INCIDENT

Uložené fragmenty L2-L7 vrstev a metadata

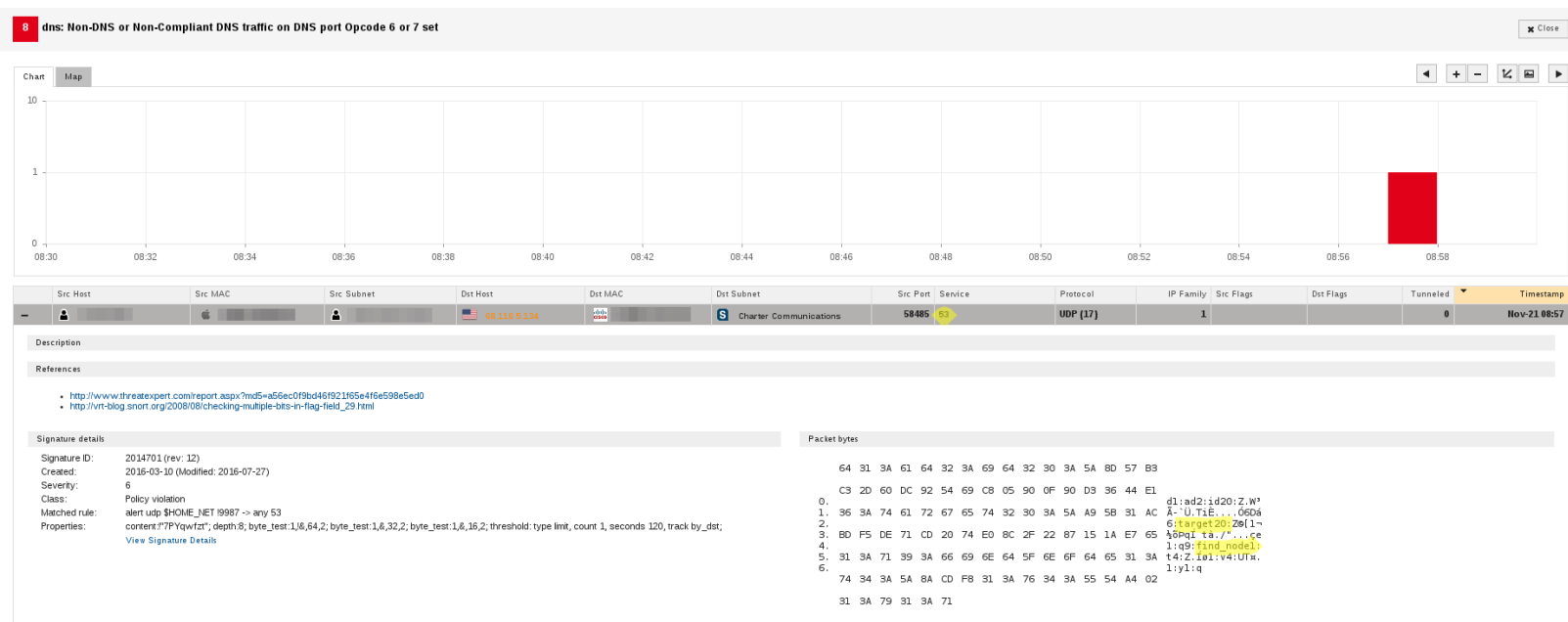
- Příznaky
- Aplikace
- Jména souborů
- Statusy odpovědí
- Hlavičky a otisk obsahu
- Tunely
- etc.

Packet bytes

```
0. 16 03 03 00 3E 02 00 00 3A 03 03 7F C1 13 57 26 .....>.....Á.Ws
1. D0 30 56 88 6E 49 4D 7E CB 21 A7 F8 BF 30 3B 41 B0V.nIM-E!g0;A
2. 92 21 DE 88 29 5B EC F2 E4 AB C4 00 C0 2F 00 00 .!P.)[àü«Ä.Ä/..
3. 12 FF 01 00 01 00 00 0B 00 04 03 00 01 02 00 0F .ÿ.....
4. 00 01 01 16 03 03 01 CC 0B 00 01 C8 00 01 C5 00 .....ÿ...È..Á.
5. 01 C2 30 82 01 BE 30 82 01 27 A0 03 02 01 02 02 .Ä0..%0...'.....
6. 09 00 98 4F 8E 13 CE 0F E6 A2 30 0D 06 09 2A 86 ...O...î.es0...+.
7. 48 86 F7 0D 01 01 05 05 00 30 23 31 21 30 1F 06 H.÷.....0#1!0..
8. 03 55 04 03 13 18 77 77 77 2E 62 34 6E 35 6F 7A .U....www.b4n5oz
9. 35 32 73 6A 65 71 6F 75 34 76 2E 63 6F 6D 30 1E 52sjeqou4v.com0.
10. 17 0D 31 37 30 31 31 37 30 30 30 30 30 30 5A 17 ..1701170000002.
11. 0D 31 37 30 38 31 38 30 30 30 30 30 30 5A 30 1F .17081800000020.
12. 31 1D 30 1B 06 03 55 04 03 13 14 77 77 77 2E 33 1.0...U....www.3
13. 73 33 68 69 32 71 65 70 61 33 64 2E 6E 65 74 30 s3hi2qepa3d.net0
14. 81 0F 20 0D 06 00 23 8F 48 8F 57 0D 01 01 01 0F
```

... PŘI ANALÝZE

Komunikace přes DNS tunel na IP adresu se špatnou reputací v Číně

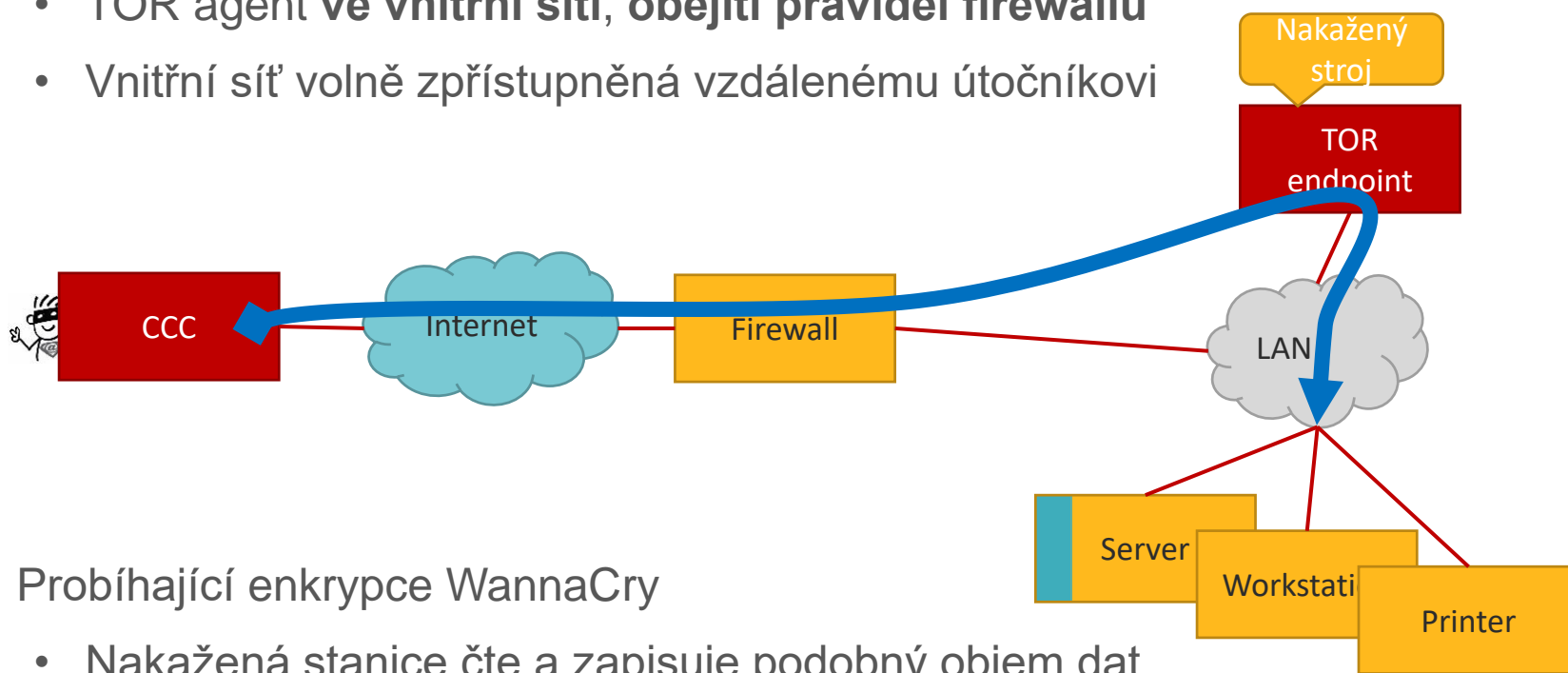


MENDEL: Co jsi našel?

Ve skutečných sítích během první hodiny od spuštění

REZIDENTNÍ MALWARE

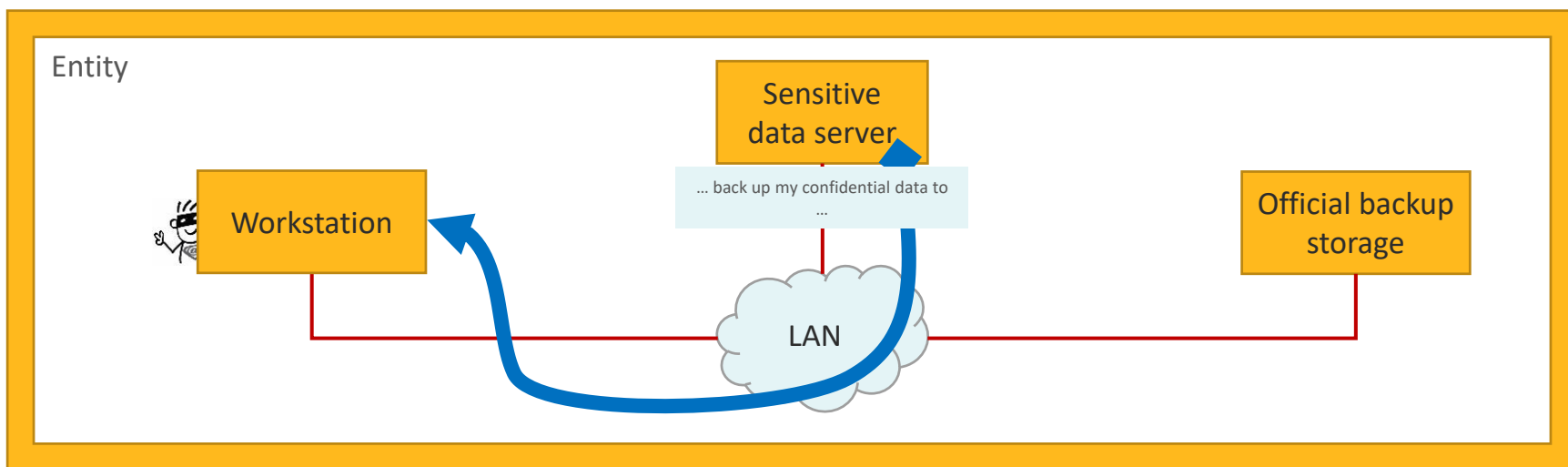
- VPN Filter
 - TOR agent **ve vnitřní síti, obejití pravidel firewallu**
 - Vnitřní síť volně zpřístupněná vzdálenému útočníkovi



- Probíhající enkrypce WannaCry
 - Nakažená stanice čte a zapisuje podobný objem dat

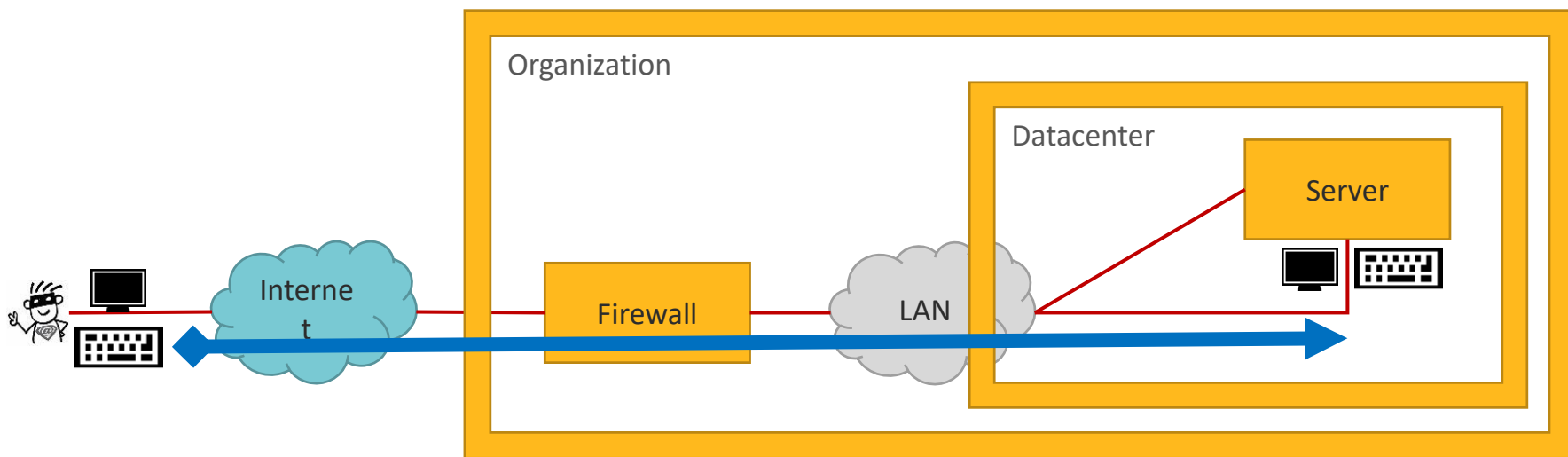
ZÁLOHOVÁNÍ CITLIVÝCH DAT NA NESPRÁVNÝ CÍL

- Konfigurace zálohování použitá při testování nebyla následně opravena a citlivá data (záznamy pacientů) končila na pracovní stanici uživatele.



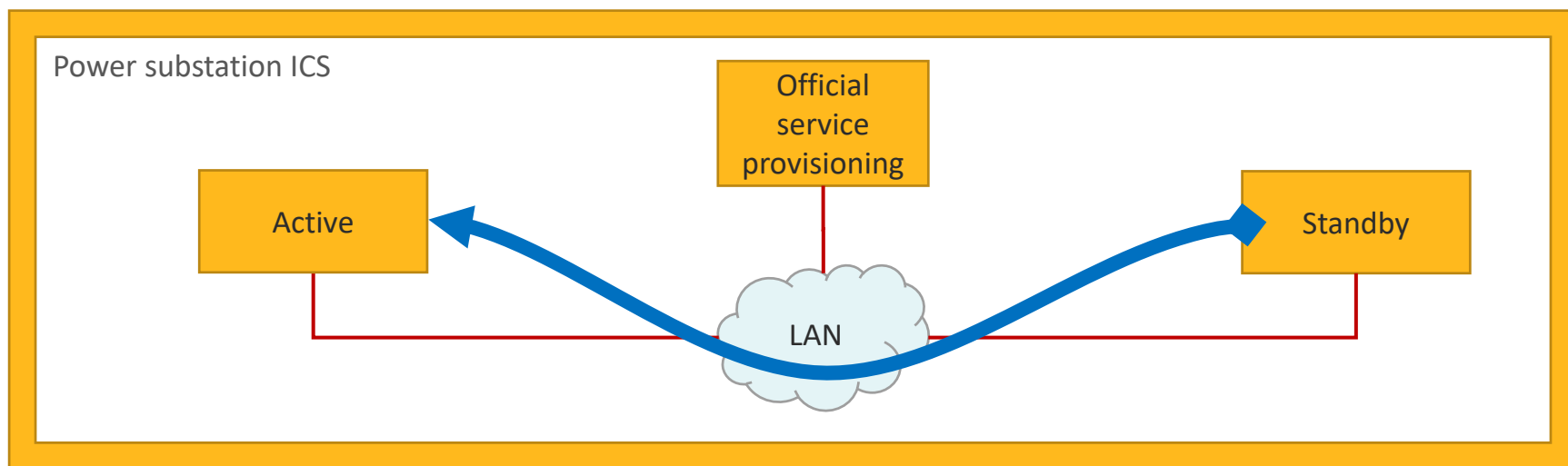
VZDÁLENÁ KONZOLA SERVERU VOLNĚ PŘÍSTUPNÁ Z INTERNETU

- Firewall nakonfigurovaný pro předávání portů na adresu serverového IPMI
- Vznikl tak neomezený přístup s možností instalovat software, navíc nebylo změněno výchozí heslo výrobce



CHYBNÁ KONFIGURACE TRAFOSTANICE

- Aktivní a záložní systém si vzájemně poskytovaly služby namísto komunikace s určeným systémem. Vzniklo riziko nesprávné funkce a ohrožení dodávky energie.

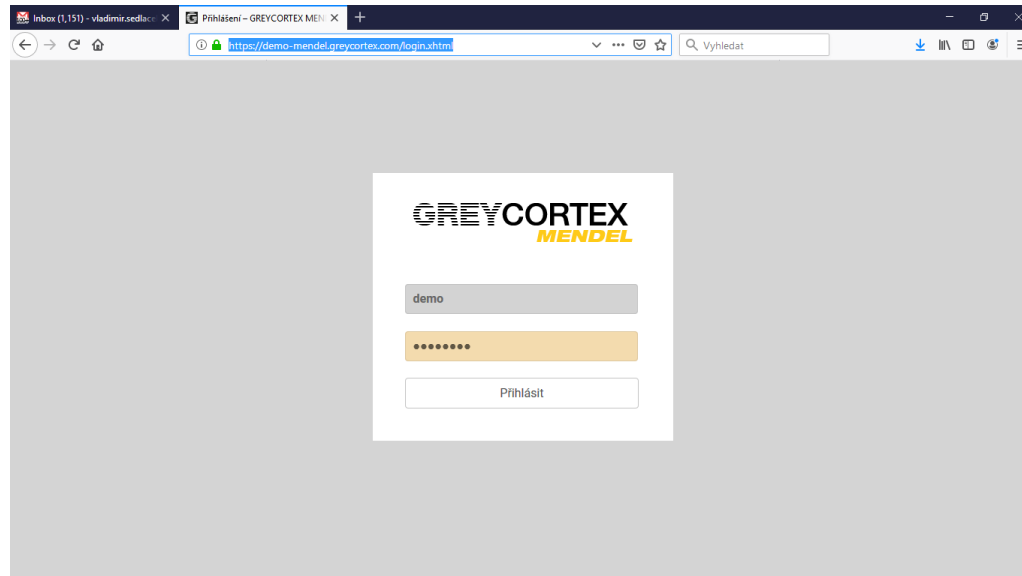


MENDEL: Tak to ukaž!

Demo, pokud se na něj dostanu...

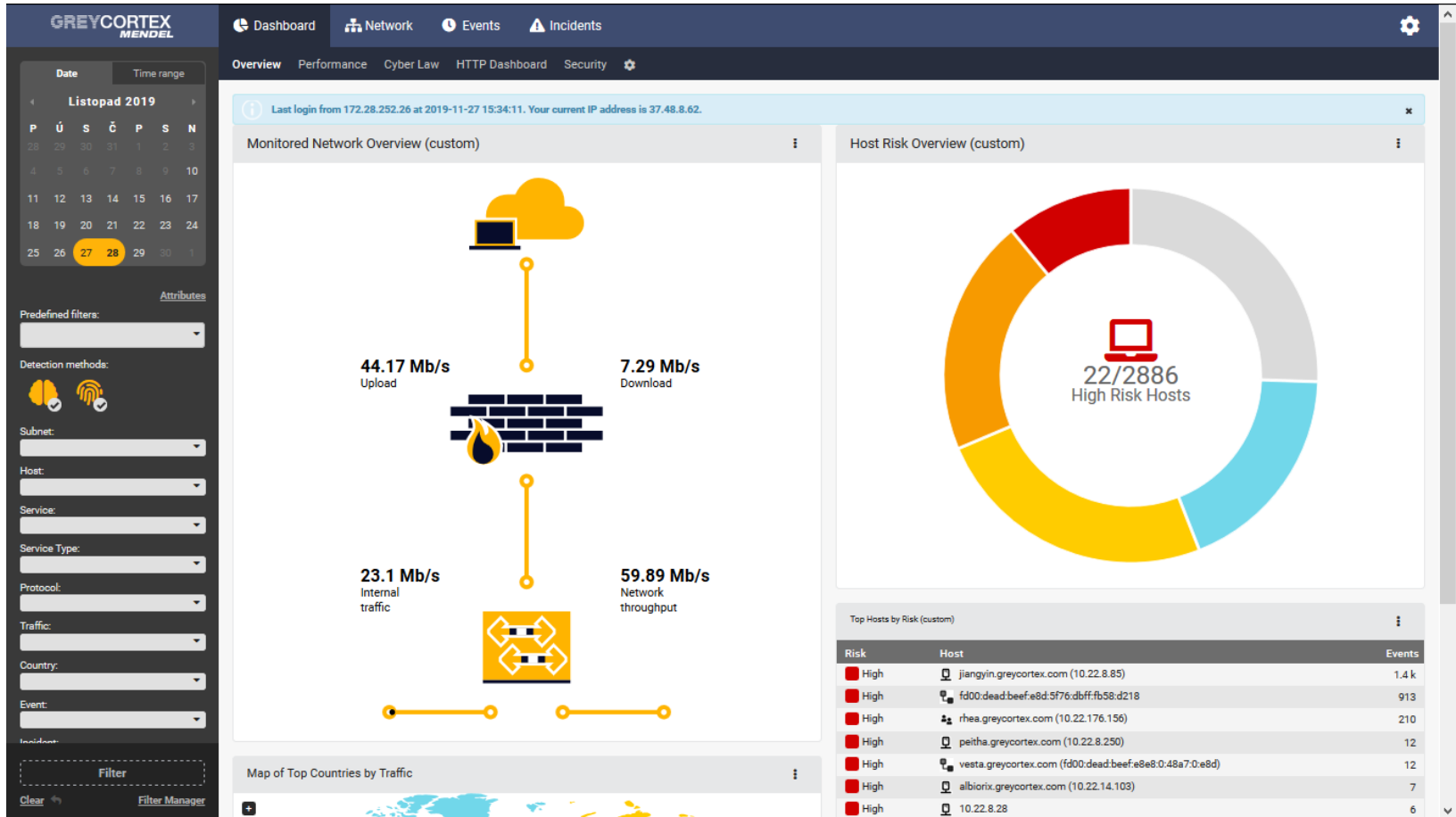
CONTINUE HERE

<https://demo-mendel.greycortex.com/>



GREYCORTEX

DEMO DASHBOARD



CASE 1 – LETHIC SPAMBOT

A Device in the Observed Network:


Queried external DNS servers (Google) for known-infected server names

Communicated via port 1123 to servers in Norway

Silenced traffic when the device was running anti-virus scanner and remained silent for the next two hours, later resuming communication on port 1123

Communicated periodically to MS Hotmail service on port 25/tcp

CASE 1 – LETHIC SPAMBOT

<i>Unsupervised Learning</i>	<i>Machine Behavior</i>	<i>Flow-based Detection</i>	<i>Discovery Analysis</i>	<i>Other</i>
Outlier: high number of communication peers & flows	SMTP Permanent Communication Anomaly: Communicated periodically to MS Hotmail service on port 25/tcp		A new service on a host discovered	IDS rule matched (Lethic SpamBOT) External DNS server, poor reputation Ips High external DNS traffic (1-2 queries reached170)

Srp 17 08:30 Srp 17 12:30 Srp 17 16:30 Srp 17 20:30 Srp 18 00:30 Srp 18 04:30 Srp 18 08:30 Srp 18 12:30 Srp 18 16:30

Host: Radka-PC

Src Host	Src MACs	Dst Host	Dst Subnet	Service	Service Type	Flows	Packets	Data	Data	Timestamp
+ 10.9.168.38	1	109.236.82.99		1123			149	81.6 k	73.3 k	133
- 10.9.168.38	1	217.23.13.94		1123			10	618	35	13

Source

1 Ports TCP 1123
[Show source ports](#)

Destination

Flow	Link layer	Network layer	Transport layer	Application Layer
Protocol: TCP				
Source		Destination		
Flags: ACK(30) PSH(23) SYN(1)		ACK(46) PSH(22) SYN(1)		
Port: 49330		1123		
	Average	Minimum	Maximum	
UET (User experience time):	2.28 s ±2.83 s	0.045 s	7.60 s	
RTT (Round trip time):	0.164 s ±0.098 s	0.026 s	0.276 s	
ART (Server application response time):	115.66 s ±11.28 s	74.00 s	119.88 s	

+ 10.9.168.38	1	217.23.14.93	1123			285	267.1 k	251.5 k	202
+ 10.9.168.38	1	217.23.10.118	1123			6	366	25	9
+ 10.9.168.38	1	93.190.140.73	1123			7	432	25	10

outlier: Peers at Subnet Services



CASE 2 – ETERNAL BLUE

A Device on the Observed Network:

Suddenly used a DNS tunnel and TOR network together, exchanging one message

After 4 hours of waiting, it started opening port 445/tcp connections on multiple external hosts

Tried to use CVE-2017-0143 (exploit MS17-010) on the connected host

CASE 2 – ETERNAL BLUE

<i>Unsupervised Learning</i>	<i>Machine Behavior</i>	<i>Flow-based Detection</i>	<i>Discovery Analysis</i>	<i>Other</i>
Outlier: high number of communication peers & flows		Network scan 445/tcp to internet		Correlation rule matched: malware spreading to internet IDS rules matched: DNS tunnel, TOR A day after updated IDS rule matched: Eternal Blue (based on CVE-2017-0143, exploit MS17-010)

CASE 2 - DEMO

9 correlation: Malware spreading

7 exploit: ETERNALBLUE Exploit M2 MS17-010

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	ΣData	ΣData	ΣEvent	Da
192.168.1.192	109.188.136.189	Private C (192.168.0.0/16)	PJSC MegaFon	445	TCP (6)						Thu 02:12:28

Reported timestamp: 2017-09-28 02:10:49 - 2017-09-28 03:12:27

Src Host	Dst Host	Protocol	Dst Port	Service	Src Packet Count	Src Packet Length	Dst Packet Count	Dst Packet Length	Src Flags	Dst Flags	End Time
192.168.1.192	109.188.136.189	TCP	445	SMB2	108	62.9 k	96	6.5 k	...AP.SF	...APRS.	2017-09-28 02:12:28

Source

- 192.168.1.192
- Private C (192.168.0.0/16)
- 52:54:00:1f:bd:7a

Destination

- 109.188.136.189
- PJSC MegaFon
- d4:a1:48:67:b8:25

Flow: Link layer | Network layer | Transport layer | Application Layer

Service: SMB2

Applications:

Request	Response
Status: 0 Command: NEGOTIATE Flags: 0 NextCommand: 0 MessageId: 0 ProcessId: 0 TreeId: 0 SessionId: 0	Status: 0 Command: NEGOTIATE Flags: 0 NextCommand: 0 MessageId: 0 ProcessId: 0 TreeId: 0 SessionId: 0

ZÁKAZNÍKEM DEFINOVANÝ DASHBOARD



Detected Threat: Periodic Communication



MENDEL detected periodic communication with a supposedly legitimate IP-address. The network metadata is classified as anomalous. Most likely, the user installed software with unknown malware

7 periodic: Malware check-in on HTTP/S ? Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	Src Data	Dst Data	ΣEvent	Date
10.10.10.10	10.10.10.10	10.10.10.0/24	10.10.10.0/24	SoftLayer Technologies Inc.	HTTP (80)	TCP (6)	18	7.85 k	33.88 k		

Flows **Peers** Reported timestamp: [range] Search Flip

Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length
10.10.10.10	10.10.10.10	TCP (6)	54456	80	HTTP	6	2.37 k	2.0 k	5	423

Flow Informations

Src Name:		Metrics
Src MAC:		ART [s]:
Dst Name:	10.10.10.10	DTT [s]:
Dst MAC:	10:10:10:10:10:10	Delay [s]:
IP Family:	1	Jitter [s]:
Src VLAN ID:	1	Max Delay [s]:
Dst VLAN ID:		
Interface:	em2	
Tunneled:	0	
Start Time:	2023-08-01 10:10:10	
Duration:	227ms	
Reported Timestamp:	2023-08-01 10:10:10	
Output Type:	0	

Request

Host: 10.10.10.10
Uri: /api/v1/health

Method: GET
Protocol: HTTP/1.1

Detected Threat: Excessive Communication



This user normally communicates through 1 to 8 network services. But, the user's device tried to communicate through 39 services, and to 120 devices around the world including Brazil, Serbia, Bosnia and Herzegovina, the United States, Singapore, and Japan. No similar communication had occurred previously in the network.

outlier: Entropy (ports) at Host

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	SData	DData	SEvent	Dst
					IP (0)						

Flows	Peers	Reported timestamp	Search	Flip											
Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	ART [s]	Src Flags	Dst Flags	End Time
+		UDP (17)	54281	45430		10	640	180							
+		UDP (17)	54281	60574		10	640	180							
+		UDP (17)	54281	43910		2	128	36							
+		TCP (6)	49913	389		6	396		6	396			...A..SF	...A.RS.	
+		TCP (6)	49909	12350		22	2.74 k	1.37 k	20	2.18 k	948	0.002	...AP.SF	...AP.SF	
+		UDP (17)	54281	443		2	128	36							
+		UDP (17)	54281	443		2	128	36							
+		UDP (17)	54281	40025		5	385	155							
+		UDP (17)	54281	40022		6	516	240							
+		UDP (17)	54281	40027		10	854	394							
+		UDP (17)	54281	40018		5	390	160							
+		UDP (17)	54281	40026		5	385	155							
+		UDP (17)	54281	40005		5	430	200							
+		UDP (17)	54281	40007		6	474	198							
+		UDP (17)	54281	40029		6	462	186							
+		UDP (17)	54281	40008		6	522	246							
+		UDP (17)	54281	40036		6	468	192							
+		UDP (17)	54281	5406		2	128	36							
+		UDP (17)	54281	13671		2	128	36							

Detected Threat: Serious Policy Breach



An exposed network device administrator with an unencrypted HTTP service resulted in an illegitimate access attempt from China. This poses a high risk for penetration and misuse.

3 policy: Incoming Basic Auth Base64 HTTP Password detected unencrypted ? Close

Src IP	Dst IP	Src Subnet	Dst Subnet	Service	Protocol	Flows	Packets	IData	OData	XEvent	Date
10.10.10.10	10.10.10.10	CNCGROUP China169 Backbone	10.10.10.10	HTTP (8888)	TCP (6)						May 11 2019 10:30

Flows Peers

Reported timestamp: Search Flip

Src Host	Dst Host	Protocol	Src Port	Dst Port	Service	Src Packet Count	Src Packet Length	Src Data Length	Dst Packet Count	Dst Packet Length	Dst Data Length	RTT [s]	Src Flags	Dst Flags	End Time
10.10.10.10	10.10.10.10	TCP (6)	59842	8888	HTTP	5	481	185	4	648	396	0.404	...AP.SP	...AP.SP	May 11 2019 10:30

Flow Informations

Src Name:
Src MAC:
Dst Name:
Dst MAC:
IP Family: 1
Src VLAN ID: 1
Dst VLAN ID: 1
Interface: em2
Tunneled: 0
Start Time:
Duration: 1s 320ms
Reported Timestamp:
Output Type: 0

Metrics

ART [s]: 0.007
DTT [s]:
Delay [s]:
Jitter [s]:
Max Delay [s]:
Signatures: 2006402, 2010019

Request

Host:
Uri:
User-Agent: Mozilla/3.0 (compatible; Indy Library)
Method: GET
Protocol: HTTP/1.1

Response

Status: 404
Content-Type: text/html

MENDEL: Co nám dává AI!

Jak to vidí zákazníci

AI V PRODUKTU MENDEL

Je to náš výkonný kolega, který nikdy nespí a pomáhá nám chránit se před kybernetickými útoky

Ukáže nám rychlé i pomalé útoky, skrytý provoz i vytrvalé hrozby

AI nás rychle zorientuje a vyhodnotí nám velké objemy nesouvislých dat

Soustředíme se na významné nálezy, vidíme skutečně odhalené hrozby

Takže my můžeme klidněji spát!



GREYCORTEX



[Tato fotka](#), unknown author, 2019-06-21 18:04,
CC BY-NC



[Tato fotka](#), unknown author, 20190727-17:56,
[CC BY-SA](#)



[Tato fotka](#), unknown author, 20190727-17:56,
[CC BY-NC-ND](#)

Děkuji za pozornost!

Vladimír Sedláček, CTO

vladimir.sedlacek@greycortex.com

GREYCORTEX